CLAIMS

What is claimed is:

- 1 1. A method comprising:
- 2 measuring a trusted original portion of firmware;
- 3 securely storing the measurement of the trusted original portion of firmware;
- 4 measuring an unqualified current portion of firmware;
- 5 retrieving the measurement of the trusted original portion of firmware;
- 6 comparing the measurement of the trusted original portion of firmware to the
- 7 measurement of the unqualified current portion of firmware; and
- 8 if the measurements match, executing the current portion of firmware as a
- 9 trusted process.
- 1 2. The method of claim 1, wherein securely storing the measurement of the
- 2 trusted portion of original firmware comprises storing the measurement in a trusted
- 3 platform module (TPM).
- 1 3. The method of claim 2, wherein the trusted platform module is embodied as a
- 2 hardware component.
- 1 4. The method of claim 2, wherein the trusted platform module is embodied as a
- 2 software-based component.
- 1 5. The method of claim 1, further comprising:

Attorney Docket: 42P18501

- 2 enforcing a locality-based security mechanism, wherein a processor must be
- 3 operating in at least one of a given locality and a higher locality to retrieve the
- 4 measurement of the trusted portion of firmware.
- 1 6. The method of claim 1, wherein measuring the trusted original portion of
- 2 firmware comprises measuring a startup portion of one of system management
- 3 mode (SMM) firmware code and platform management interrupt (PMI) firmware
- 4 code.
- 1 7. The method of claim 1, further comprising performing a core root of trust
- 2 measurement (CRTM).
- 1 8. The method of claim 7, wherein the CRTM is a static CRTM comprising a
- 2 measurement of a trusted bootable portion of firmware.
- 1 9. The method of claim 7, wherein the CRTM is a dynamic CRTM measured via
- 2 execution of processor microcode.
- 1 10. The method of claim 1, further comprising:
- 2 creating a descriptor indicating where the trusted original portion of firmware
- 3 is located.
- 1 11. A method, comprising:
- 2 measuring at least one integrity metric corresponding to a trusted portion of
- 3 an original firmware configuration;

Attorney Docket: 42P18501

- 4 storing a respective measurement corresponding to each of said at least one
- 5 integrity metric in a corresponding platform configuration register (PCR) of a trusted
- 6 platform module(TPM); and
- sealing a secret to the TPM, the secret contained in a digest including the
- 8 secret concatenated with the respective measurement(s) stored in the PCR(s),
- 9 wherein a current firmware configuration includes a portion that matches the
- trusted portion of the original firmware configuration to unseal the secret.
- 1 12. The method of claim 11, further comprising:
- specifying a locality to be associated with a trusted firmware process; and
- concatenating the locality to the secret and the respective measurement(s)
- 4 used to form the digest stored in the PCR(s).
- 1 13. The method of claim 11, further comprising:
- 2 asserting a locality corresponding to an execution privilege level;
- 3 storing at least one of the respective measurement(s) in a PCR that may be
- 4 extended if a current execution privilege level matches or exceeds the locality of the
- 5 execution privilege level that is asserted.
- 1 14. The method of claim 12, wherein the locality is locality 1.
- 1 15. The method of claim 11, wherein the trusted portion of the original firmware
- 2 configuration includes a trusted boot block.
- 1 16. The method of claim 15, further comprising:
- 2 measuring the trusted boot block to obtain a core root of trust measurement
- 3 (CRTM).

- 1 17. The method of claim 11, wherein the trusted portion of the original firmware
- 2 configuration includes a startup portion of one of system management mode (SMM)
- 3 firmware code and platform management interrupt (PMI) firmware code.
- 1 18. The method of claim 11, further comprising:
- attempting to unseal the secret sealed to the TPM; and
- 3 executing firmware as a trusted process if the secret is unsealed, otherwise
- 4 executing the firmware process as an untrusted process.
- 1 19. The method of claim 11, wherein the integrity metric is measured by
- 2 executing microcode on a processor.
- 1 20. An article of manufacture, comprising:
- a machine-readable medium have instructions stored thereon, which when
- 3 executed perform operations including:
- 4 measuring a trusted portion of an original set of firmware components during
- 5 a pre-boot phase of a computer system;
- 6 storing the measurement of the trusted portion of the original set of firmware
- 7 components in a trusted platform module (TPM) platform configuration register
- 8 (PCR);
- 9 measuring a portion of a current set of firmware components during an
- operating system (OS)-runtime phase of the computer system
- determining if the measurement of the portion of the current set of firmware
- 12 components matches the measurement of the portion of the original firmware
- 13 components; and

Attorney Docket: 42P18501

- providing indicia to a processor to execute the portion of the current set of
- 15 firmware components as a trusted process if the measurements match.
- 1 21. The article of manufacture of claim 20, wherein each of the original and
- 2 current sets of firmware components correspond to system management mode
- 3 (SMM) firmware.
- 1 22. The article of manufacture of claim 20, wherein each of the original and
- 2 current sets of firmware components correspond to platform management interrupt
- 3 (PMI) firmware.
- 1 23. The article of manufacture of claim 20, wherein the machine-readable
- 2 medium comprises further instructions to perform the operation of performing a core
- 3 root of trust measurement (CRTM).
- 1 24. The article of manufacture of claim 20, wherein the machine-readable
- 2 medium comprises further instructions to perform operations including:
- sealing a secret to the TPM, the secret contained in a digest including the
- 4 secret concatenated with the measurement of the trusted portion of the original set
- 5 of firmware that is stored in the PCR.
- 1 25. The article of manufacture of claim 20, wherein the article comprises a flash
- 2 device.
- 1 26. A system comprising:
- 2 a processor, including microcode instructions;
- memory, operatively coupled to the processor;

4	a trusted platform module, operatively coupled to the processor; and
5	a flash device having firmware instructions stored thereon, which when
6	executed on the processor perform operations including:
7	retrieving a first measurement stored in the TPM, the first
8	measurement comprising a measurement of a trusted portion of the firmware
9	instructions;
10	measuring a current portion of firmware instructions analogous to the
11	trusted portion of the firmware instructions to obtain a second measurement;
12	comparing the first measurement to the second measurement; and
13	if the first and second measurements match, programming the
14	microprocessor to execute the current portion of firmware instructions as a
15	secure process.

- The system of claim 26, wherein the microcode instructions may be executed to perform the operations of generating a dynamic core root of trust measurement
- 3 (CRTM) for the system.
- 1 28. The system of claim 26, wherein the microcode instructions may be executed 2 to perform operations including:
- measuring the trusted portion of the firmware instructions to produce the first measurement; and
- storing the first measurement in a platform configuration register (PCR) of the TPM.
- 1 29. The system of claim 26, wherein, wherein each of the original and current
- 2 sets of firmware components correspond to system management mode (SMM)
- 3 firmware.

- 1 30. The system of claim 26, wherein, wherein each of the original and current
- 2 sets of firmware components correspond to platform management interrupt (PMI)
- 3 firmware.